A Historical Perspective . . .

THE U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND'S TECHNOLOGY INTEGRATION CENTER

————————

James H. Ward

————————

Introduction

In terms of impact, no single system, strategy, or focus in the Army has been a greater change agent than computers and the networks that have linked them. In fact, as early as 1984, U.S. Army Information Systems Command (ISC) officials forecast the Army's growing reliance on the computer. In so doing, they were determined to shorten the acquisition cycle while being mindful of the total cost of ownership.

In 1984, like today, new systems were being developed to replace old machines, enhance capabilities, and add staggering capacity to the Army's voice, data, and messaging processes. It was clear that the Army needed a center of excellence to test and validate its information technology (IT) capabilities and tools for integration and application within its infrastructure.

The responsibility to develop and manage such a center of excellence was assigned by ISC to the U.S. Army Information Systems Engineering Command (ISEC), which had worked for

years on computing and information management improvements. In late 1984, LTG Emmett Paige (USA, Ret.) launched the Small Computer Engineering Center (SCEC) in Fort Huachuca's Splinter Village, AZ. This facility represented a quantum leap forward in the Army's commitment to the future of information systems integration, which was sparked by the sweeping changes the personal computer (PC) was introducing to the world. In a way, it represented a kind of Manhattan Project for IT.

The Early Years

Historically, in the years following World War II, many engineers and computer scientists believed in the old acquisition cycle. Paige said they believed that the intensive "waterfall" method of design, build, test, and field had served the military well and, if it was not broken, why fix it. "There was no doubt in my mind that it was an almost impossible task to change the culture of the scientists and engineers who had come along after World War II. They wanted no part of

using commercial communications and computers on the battlefield, and that attitude also permeated the Army combat development community at Fort Gordon [GA] and the troop units in the field, … " Paige added.

With the advent of the PC, the Army needed to identify machines with the right capabilities at a time when numerous computer manufacturers were bursting on the scene. The Army also needed to support signal leaders' decisions to purchase commercially built PCs. "Our intent was that no computer would be purchased for Army use unless it had been evaluated by the SCEC. It was our intent that the project managers and program managers at Fort Monmouth, [NJ], would have a cell of experts to help and advise them in their task of providing the Army with the capabilities they needed at the lowest total cost of ownership," Paige said.

In its early days, the SCEC operated as a kind of skunk works with 20 engineers, most of them young officers and students who could get in on the ground floor of equipment testing and evaluation. Then, as they moved up in rank or position, they would be in place to influence the way technology would be used in the military.

Jo Tate Osborne, who served as SCEC's Senior Electronics Engineer and Deputy in the early years, said the center was responsible for reviewing each component of the Army's mini- and micro-computer contracts and for assisting systems engineers in selecting the most appropriate platforms for their application.

Another key member of the staff was Ron Boggie, who served in a number of capacities within ISEC and the SCEC, which later became known as the Computer Engineering Center (CEC) in 1989. Boggie believed that the "slick" advertising brochures and new product briefings that promised performance were directed more at outdistancing the competition than meeting the needs of the kind of large-scale competitive procurement the military was demanding.

Dr. Frank Jenia, ISEC's Deputy Commander and Technical Director said, "The staff knew that their evaluations

would influence the shape of information technology. We simply had to ensure that our reports were completely free of personal opinion and based solely on empirical results."

Echoing those remarks is one of ISEC's early CEC military engineers whose pioneering work led the military down the domain name server road. "All small computer software and hardware had to pass our evaluations," said MAJ Curt Vincent, who served in the CEC from 1985 to 1990. "They had to be nonproprietary. We take that for granted now, but back then, it was no fun. We had tons and tons of 'stovepipe' information systems, which could not talk to each other. Within a particular military organization, the personnel systems didn't talk to the logistics systems so data had to be entered twice or printed out and re-entered. This had to go."

The Next Phase

The leap from single-box evaluations to ensuring "systems integration" began with evaluations the team conducted on servers, routers, switches, and local area networks.

By the late 1980s and early 1990s, it became clear that the CEC would be asked to do system-of-systems or end-to-end integration testing. (In 1993, with the increase in whole systems engineering, CEC became known as the Technology Integration Center (TIC).) At first, this meant sending engineers to Army installations, setting up a parallel system to the one being used in the field, and running the evaluations.

ISEC soon realized that this method of testing at Army installations would be far too costly and disruptive to the Army. The practice of placing terminal emulators in the TIC laboratory began shortly thereafter.

"The real breakthrough came when we were able to capture all the keystrokes being used in the field under what was called Installation Transition Processing (the forerunner to Sustaining Base Information Services) and simulate on a broad scale how that system would operate. For the first time, we could see where the bottlenecks were and recommend

hardware and software fixes, Dr. Michael Gentry, the Army Signal Command's Senior Technical Director, said. By providing a place for systems evaluations, Gentry said the TIC could also help the Army look into the future with a certain high level of certainty and credibility.

Throughout its history, ISEC's TIC, now a part of the U.S. Army Communications-Electronics Command, Fort Monmouth, NJ, has served as DOD's information technology gatekeeper.

"Everyone in the vendor community knows that if they want to sell a product to the Army, they should make plans to work with ISEC and get their box on our evaluation schedule. Most of them know this and, because of our reputation, they want to do business the TIC way," Jenia said.

And what is "the TIC way?" According to Jenia, the TIC staff also acts as an innkeeper. They are responsible for maintaining the laboratories, test equipment, computers, networks, and facilities in a ready state to emulate any Army infrastructure for complete and unbiased evaluations. In computer-technology terms, this also means having access to the full intellectual capacity of the ISEC, with its critical-skill engineering experts in all areas of technology. The TIC can then provide the Army and the vendor the empirical evidence required to shorten the acquisition cycle at dramatically lower cost and risk to the government.

According to Tate, the TIC is respected throughout the Defense establishment as an organization that has changed the way computing is done—at every Army post, camp, and station.

According to Paige, the value of the TIC continues to grow because it has stayed close to its original charter of being the one place in the Defense community where IT professionals can go to get a true picture of the system they are working on. This includes gigabit Ethernet (which will help greatly speed up traffic flow on the installations' campus area networks), modeling and simulation, public key infrastructure, security, knowledge management, multimedia, voice and data over Internet protocol, and

other applications and technologies.

The TIC also supports the Army by evaluating the functions of the Common User Installation Transport Network at all Army camps, posts, and stations. To this end, the TIC emulates such state-of-the-art information infrastructure components as routers, switches, hubs, and concentrators. This process also involves work with other ISEC engineers who troubleshoot network and system problems throughout the command and the Army.

Conclusion

Not only has the TIC grown in size, Paige said, it has grown in importance to both the Army and DOD. "When I was the Assistant Secretary of Defense for C3I [Command, Control, Communications, and Intelligence], I fully supported the relationship between the TIC and such other DOD agencies as the Joint Interoperability Test Command [at Fort Huachuca]," Paige said.

The ISEC's TIC has added to the military's ability to get the right box thoroughly evaluated and into the hands of the end user prior to fielding.

"We've been able to leverage the expertise of ISEC and combine this with the fact that the TIC holds the reputation as the top lab of its kind to really change the whole nature of information technology. Members of ISEC evaluate and design integrated commercial information technology we use out there, and that's significant," Jenia said.

JAMES H. WARD is a Research Analyst for ISEC, Fort Huachuca, AZ. He is a former Army Public Affairs noncommissioned officer with a B.S. in government and politics from the University of Maryland.